

Castellum Labs

Corporate Presentation



About Us

Castellum Labs

New Age Cyber Security Company

Based in Hyderabad, India
with global customers

Services & Platforms at Cross
Section of Intel, Monitoring &
Simulations

Strong Handpicked Team of
50+ with (best of security
talent globally)

Started by people with
decades of product & CySec
exp

Subscription Modeled &
Globally Delivered CySec
Services

Value + Impact from Day
One, No Installation & No
Deployment



Rajeev Shukla, Founder

- 27 years building technology businesses
- Leadership roles in Sun, CA, Quark & more
- Wide experience across US, India and Europe
- Founded Castellum Labs over three years back
- Commercially successful product/service portfolio

Current Customers in

- India
- Australia
- Middle East
- USA
- UK

Current Customer Segment

- SaaS Product Companies
- Financial and Banking
- E-Comm Player
- Telecom
- Retail

Served Customer in following Areas

- Application Security & Governance
- ISO 27K & GDPR readiness preparation
- Red Teaming. Active Defense Assessment
- Threat Intelligence and Threat Management
- SOC Monitoring (Managed Detection & Response)
- Cloud Security Designing and Cloud Security Governance

Threat Landscape of 2022 is “Different”

Almost all of the attacks use large automated infra

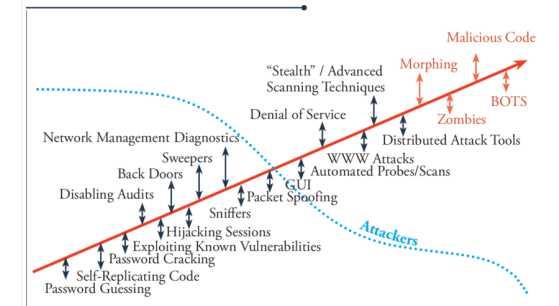
Cyber criminals do not need to be hacking experts

Time to exploit a vuln or a misconfigs reducing everyday

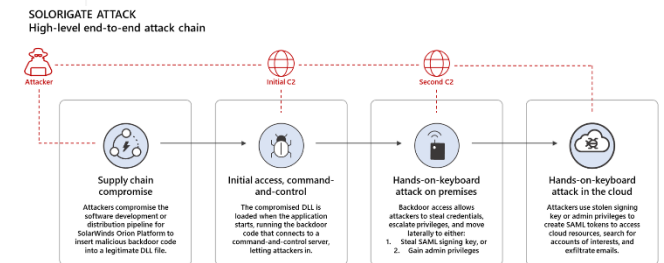
Large scale malicious traffic can be generated through automated infrastructure

*Ransomware as a service
Exploit code on darkweb
Hackers on rental hire*

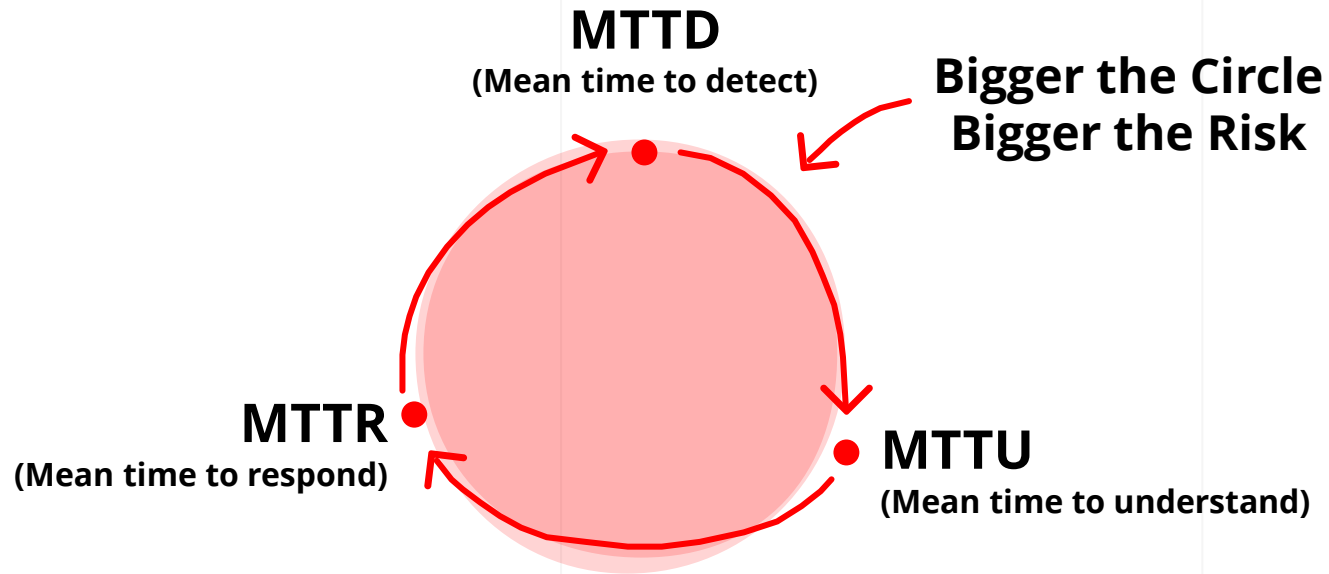
It takes mins and hours to get a vulnerability or gap to be exploited, not days/weeks



Ever Evolving Cyber Attack Models



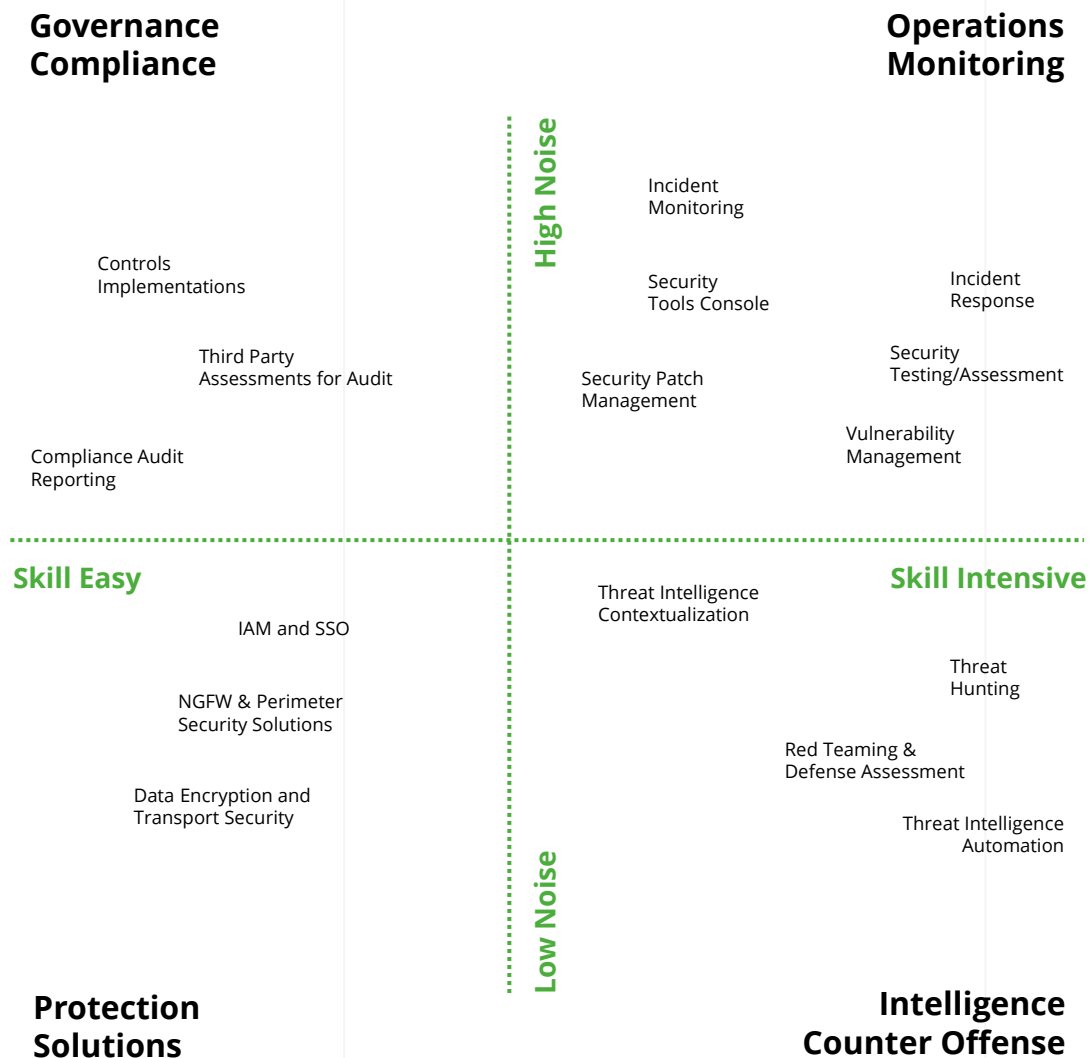
• Time to Respond @ Center Stage



- Vulnerabilities
- Network & Web Attacks
- Internal Malicious Activities
- Org's Stolen and Breached Data
- Backdoors & Exploits in IT Setup
- Fake and Fraud Assets & Activities



Threat Management, is Complex



Near Real Time or Real Time detection and response capabilities are difficult achieve and maintain

Vulnerabilities and defense gaps closure is subjective and is slow because of silos & lack of automation

CISOs view of his own org's cyber security is fragmented and incomplete. It also lack a unified perspective

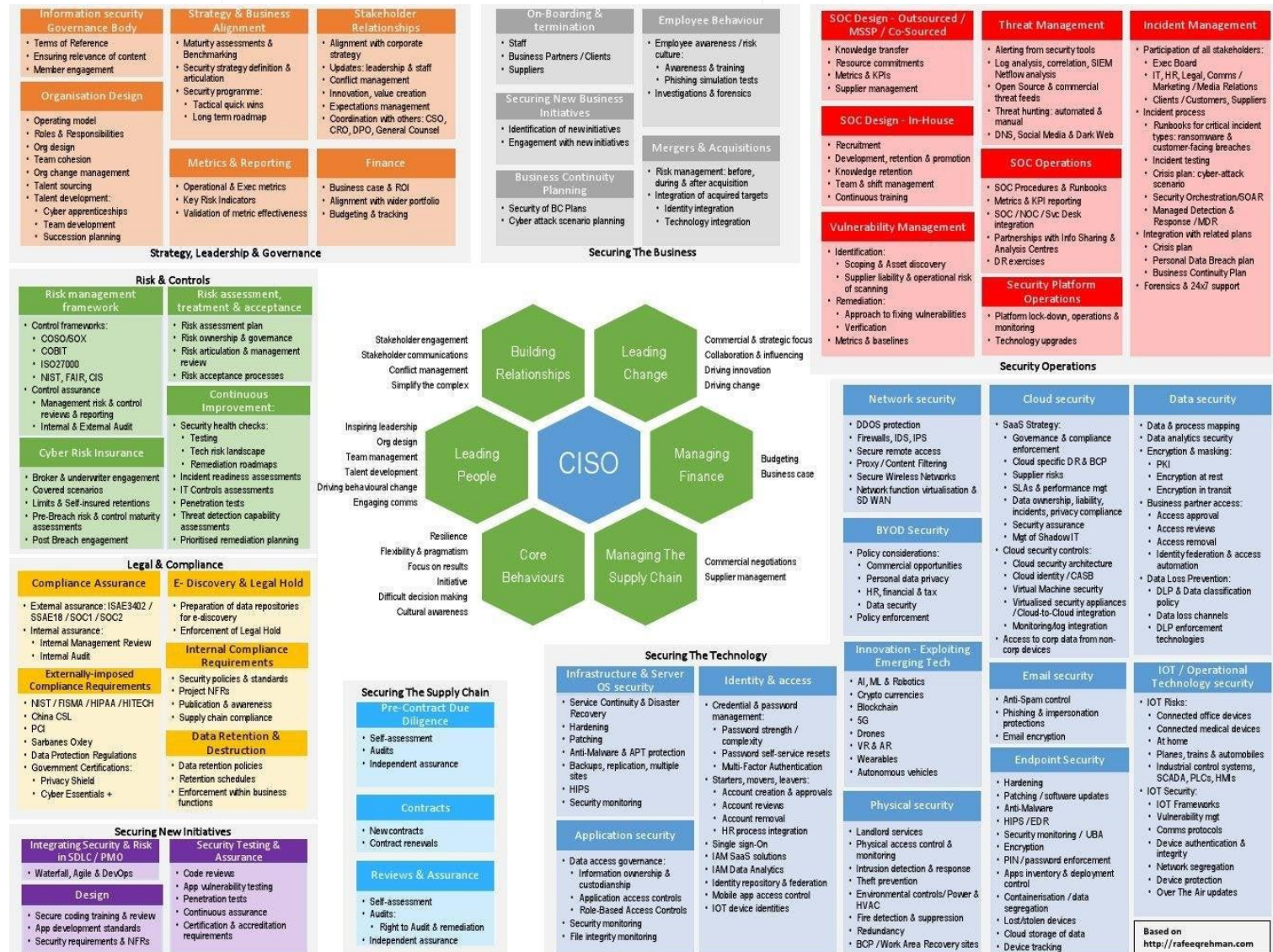


CISO Role 2022

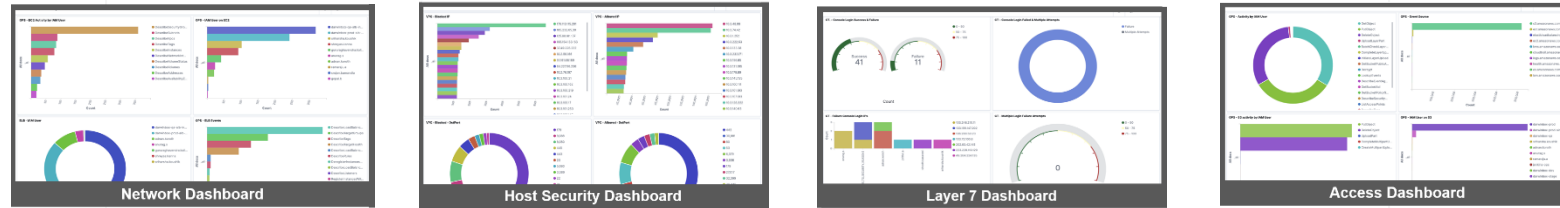
Dealing with dozen of products across spectrum of cyber security

Conflicting priorities leading to clutter and confusion in threat management

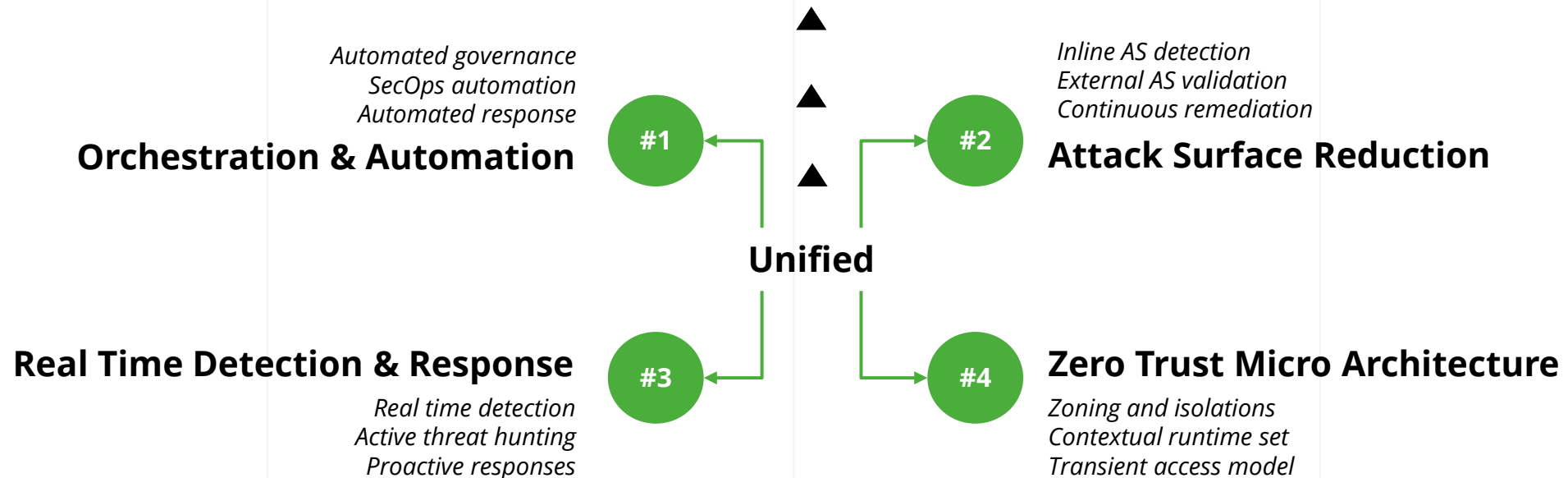
Organizational silos and operational challenges creating real time action difficult



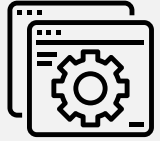
CLabs' Vision is "Clarity" & "Defense in Depth"



We create **Single Pane of Glass** visibility for YOU!



Castellum Cyber Security Services



Application Security

Managed AppSec Programs



Cloud Security

Cloud Security Design & Governance



Threat Intelligence

Intel Enriching, Automation & Hunting



Enterprise Assessments

End-to-End Security Assessments



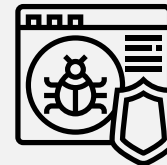
SOC Monitoring

Managed Detection and Response



Vulnerability Management

Enterprise Vulnerability Orchestration



Threat Simulations

Red Teaming & Breach Simulations



Certifications

ISO 27K & GDPR Readiness

• Our Technology Platforms



Our SaaS platform for darkweb monitoring, external threat discovery, attack surface mapping & risk management



End-to-end SOC platform for 24x7 monitoring, intel application, investigations & response management/coordination



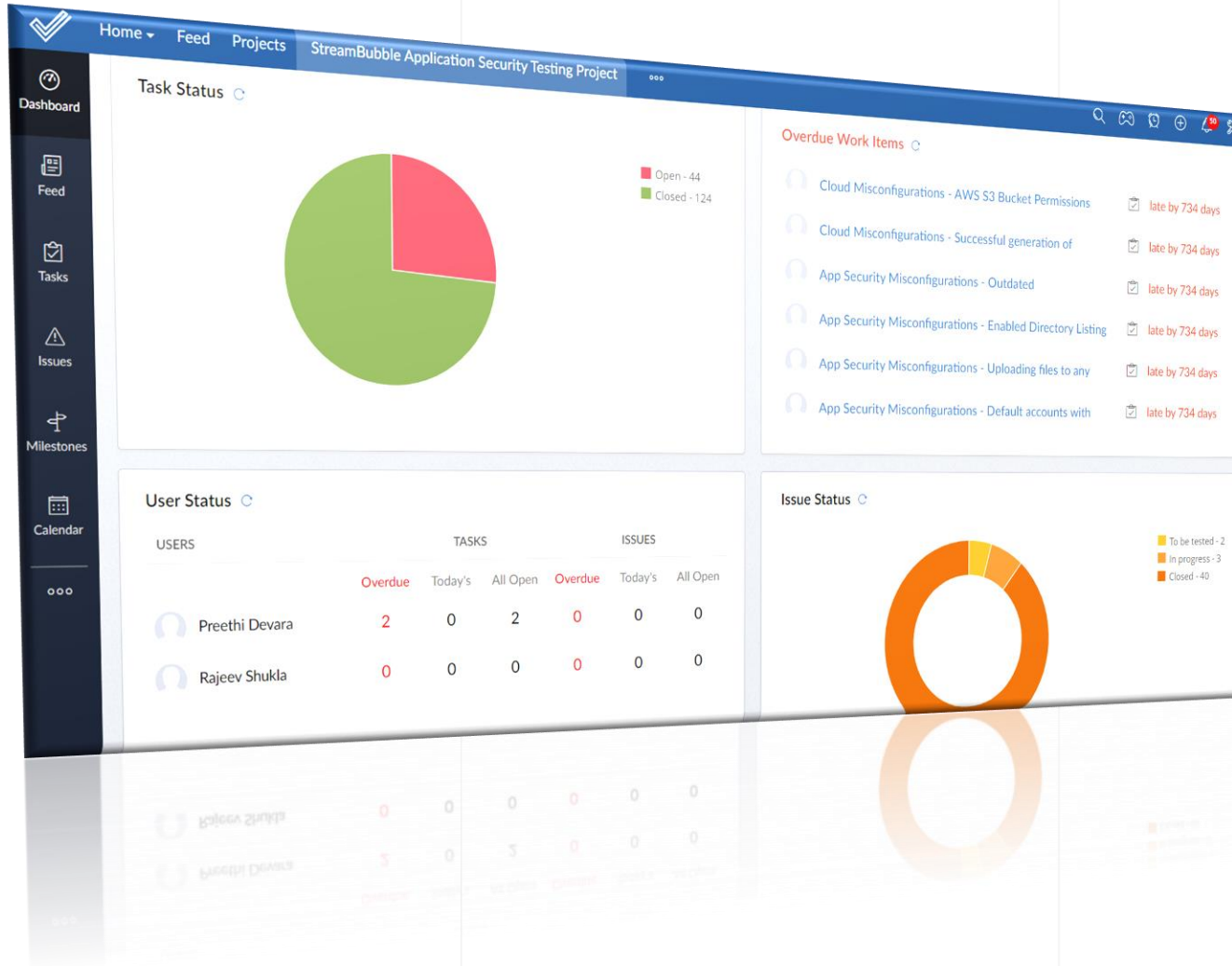
Application security platform we use to create an extraordinary customer experience for web, mobile and API security

"Our engagements, for end-to-end coordination of cyber security are powered by our cloud platforms

Our platforms enable cyber orchestration, which can not be achieved with only tools and people

An extraordinary experience and a resilient defense is delivered with help of our cutting edge platforms

Unified View <> Single Window



Castellum CySec Engagements

- “One” security portal
- All collaboration on one portal
- All progress maintained at “1” place
- Incredible dashboards and reporting
- Unified security window for customers
- Security document repository for customers

Unmatched Executions Quality

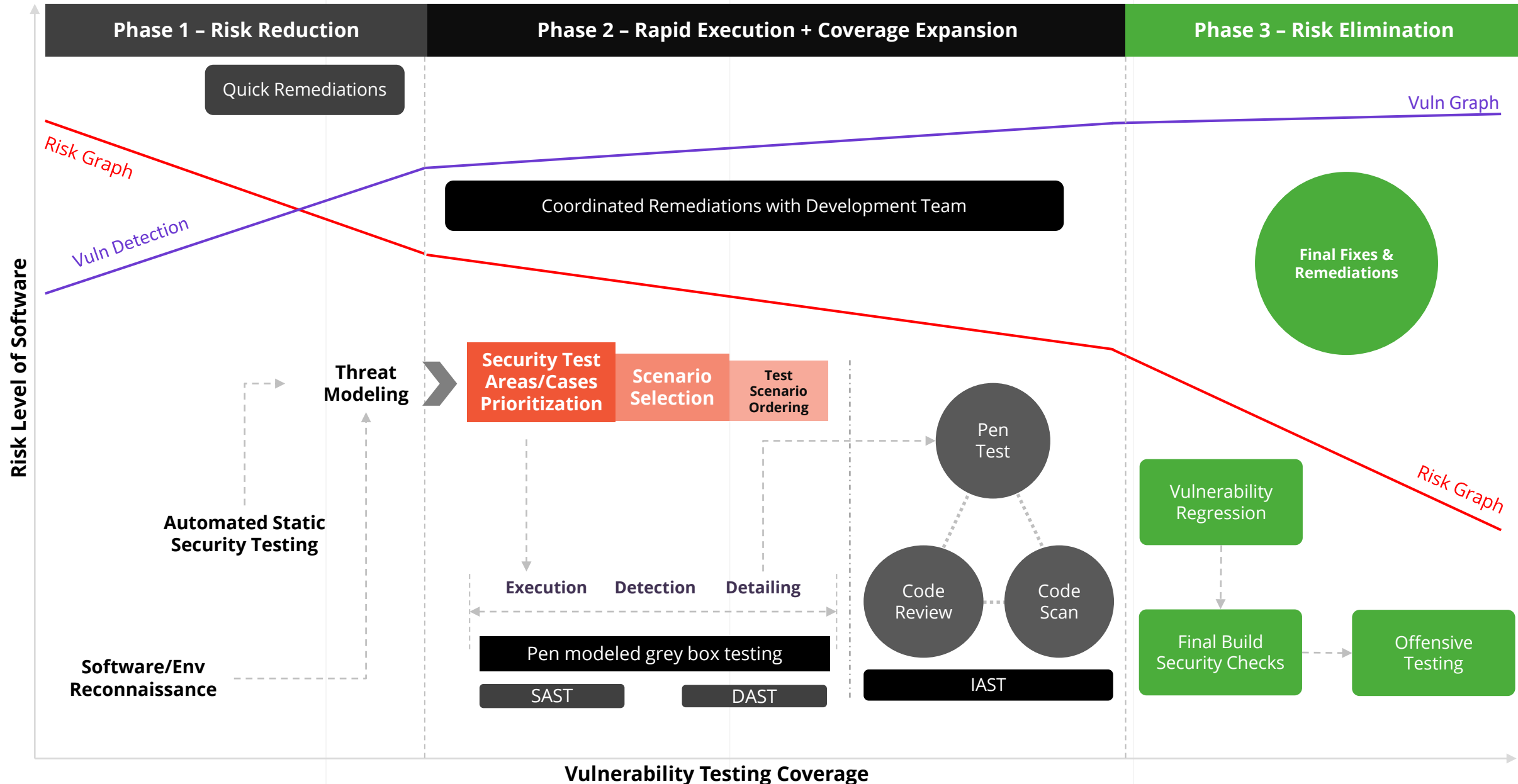


First Security Testing Run (120 Apps)			Apr							May							Jun							
			(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)	(4 Days)			
Application Category	Size	Count of Apps <i>(by Size)</i>																						
Critical Applications	Large Apps	5																						
	Medium Apps	24																						
	Small Apps	19																						
High Priority Applications	Large Apps	14																						
	Medium Apps	29																						
	Small Apps	29																						

Castellum Labs brings **Program Quality Strength** to Your Cyber Security



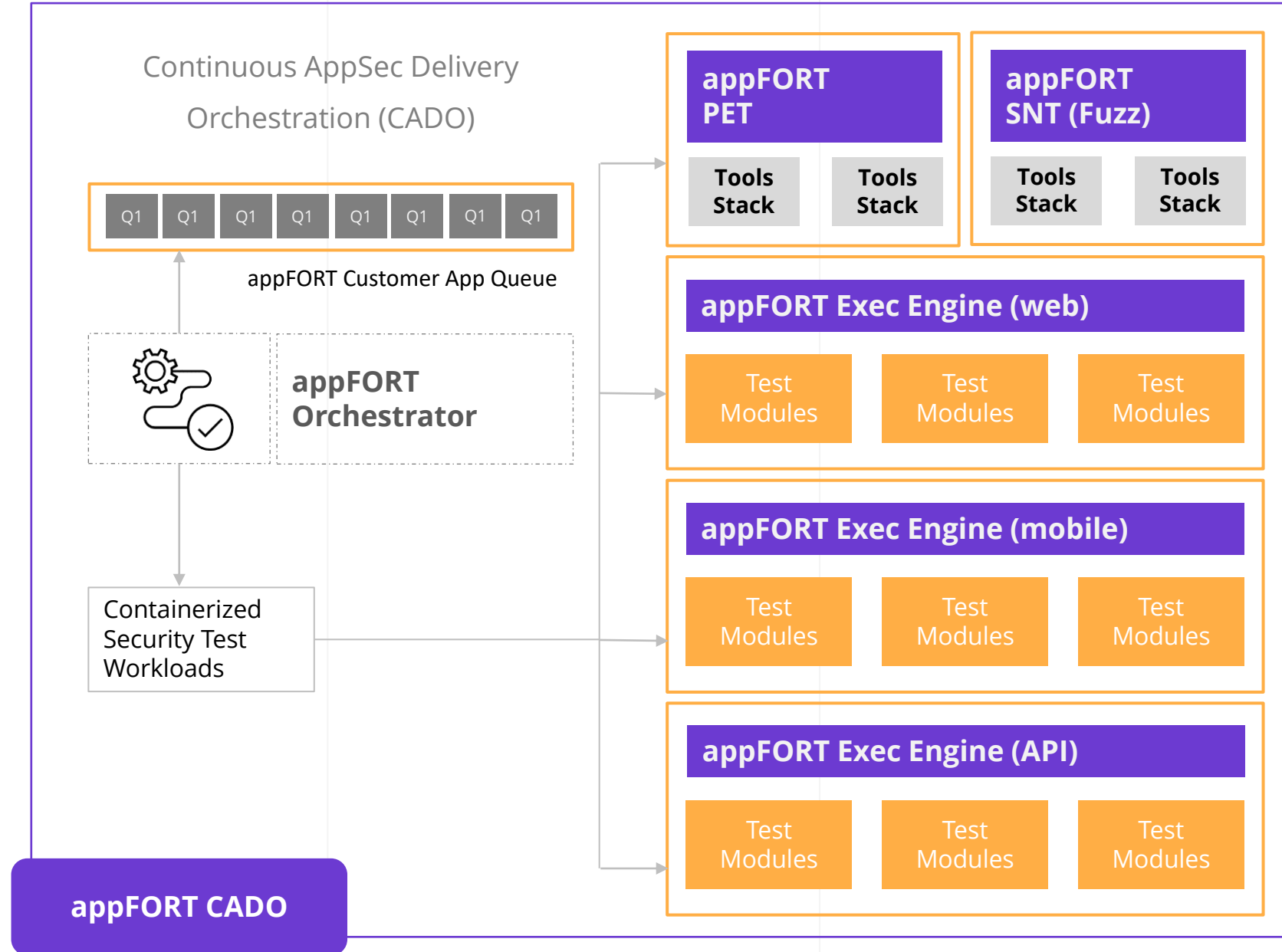
Advanced Cyber Security Frameworks



Our Platforms, Heart of Seamless Orchestration


Cloud based delivery platforms

- For Security Automation
- For Scale Orchestration
- For Execution Management
- For Continuous Checks/Testing
- For Controls and Posture Mgmt
- For Automated Threat/Risk Analysis



Deep Insights, Dashboards & Analytics

- Set of CISO dashboards
- Deep data analytics for risks
- Human assessment powered
- Built-in insights in all services
- Intel correlations for action
- Realtime on CLabs portal

AppSec Dashboard for Enterprise					Level 1 Board					
					CISO AppSec Summary					
Application Name	Risk Rating	State of Vulnerability Levels (Across Major Areas)							Software Surface Risk Rating	
	Weighted Scale 1 to 10	Authentication Areas Gaps	User/Role/Access Mgmt Gaps	Session Mgmt Weaknesses	Input Validations	Injection Protections	App Sec Misconfiguration	File Ops/Lib Inclusion		
	1 High - 10 Low									
	CRM Application	3	Critical	Critical	Medium	Medium	High	Medium	Low	4.6
Sales Management S/W	3	Critical	Critical	Critical	Critical	High	Medium	Low	Enterprise Wide AppSec Posture	
Human Resources Software	3	Low	Critical	High	Medium	Low	Critical	Critical	Critically Vuln Applications	6
Supply Chain Software	5	High	Medium	Medium	Low	Low	High	High	Apps with High Exposures	2
CRM Mobile Application	6	Medium	Medium	Low	Medium	Low	Medium	Medium	Apps with Moderate Exposure	8
Biometric Attendance Web	8	Medium	Low	Medium	Medium	Medium	Medium	Low	Secure App Surfaces	1
Financial Software	10	Low	Low	Low	Low	Low	Medium	Medium	Forified Applications	3
Leave Portal	10	Low	Low	Low	Low	Medium	Medium	Low	Vulnerability Areas with Critical Issues	
Cash Management Software	10	Medium	Low	Low	Low	Low	Low	Medium	Authentication	5
Facility Mgmt Mobile App	9	Medium	Medium	Medium	Medium	Low	Low	Low	User/Role/Access	6
Partner API (Trede Platform)	6	High	High	Medium	Medium	Low	Low	Low	Session Management	3
Enterprise Content Portal	3	Critical	Critical	Medium	Medium	High	Medium	Low	Input Validations	3
Risk Management Software	3	Critical	Critical	Critical	Critical	High	Medium	Low	Misconfigurations	1
Materials Mgmt Movable App	4	Low	Low	High	High	High	Medium	Medium	File Ops/Lib Inclusion	1
Project Web Site	7	Medium	Medium	Medium	Medium	Low	Medium	Low		
Partner Platform Web	7	Medium	Low	Medium	Low	Medium	Medium	Medium		
Partner Platform Mobile	8	Medium	Medium	Medium	Medium	Low	Medium	Low		
e-Commerce Platform	7	Medium	Low	Medium	Low	Medium	Medium	Medium		
e-Commerce Mobile App	8	Medium	Medium	Low	Medium	Low	Medium	Low		
Support Platform	3	Critical	Critical	Critical	Critical	High	Medium	Low		



Security as a Service In True Form

Various Platforms

Supported by people in
Bangalore, Hyderabad and Pune



Cloud based Labs

All work in our engagement is
done from secure cloud labs



Subscription

Available as a subscription or
annual contract, with real ROI

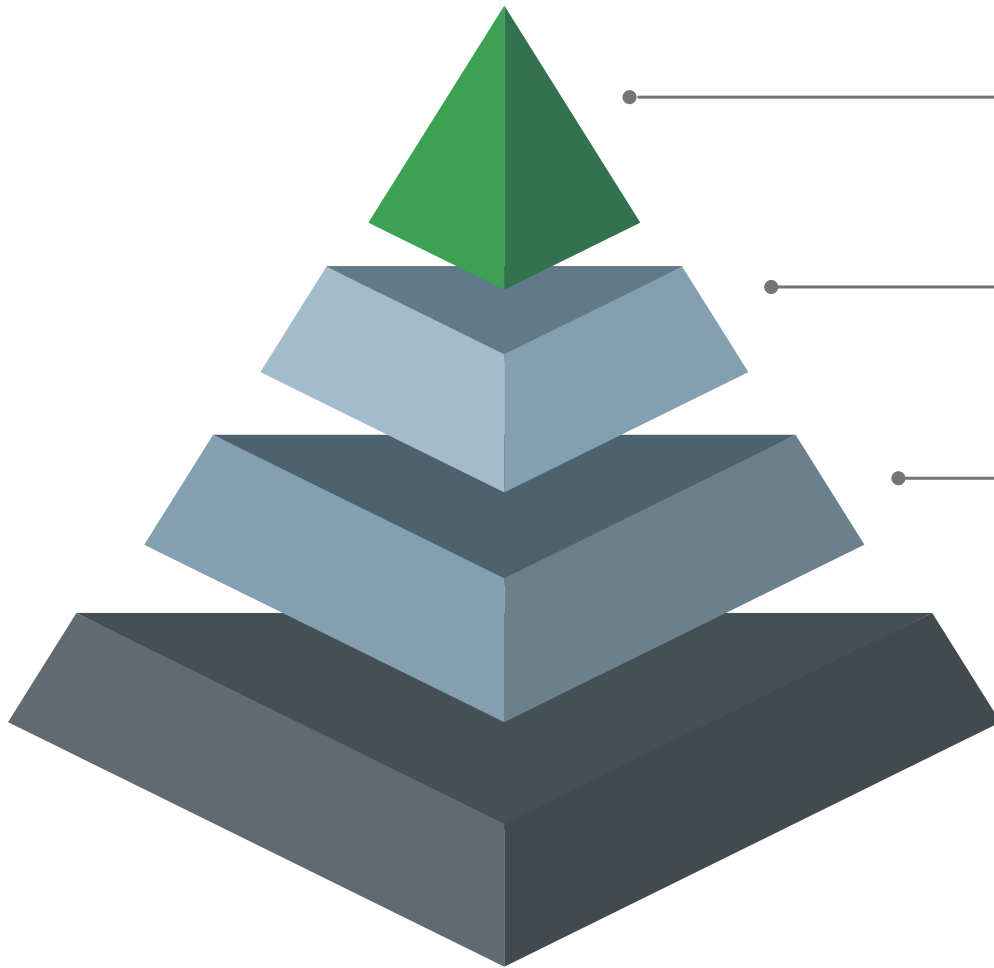


Beyond Reporting

Human assessment, automation
and strategic posture shift

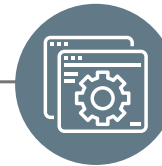


Contextual, Progressive & Continuous



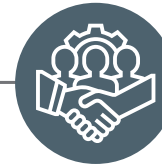
Ultimate:

Single-pane-of-glass security control with Automated and Assisted proactive and reactive incident response



Advanced:

External Threat Monitoring (**watchOUT**)
Managed Detection and Response (**threatNiXD MDR**)
Secure Applications (**appFORT**)



Recommended:

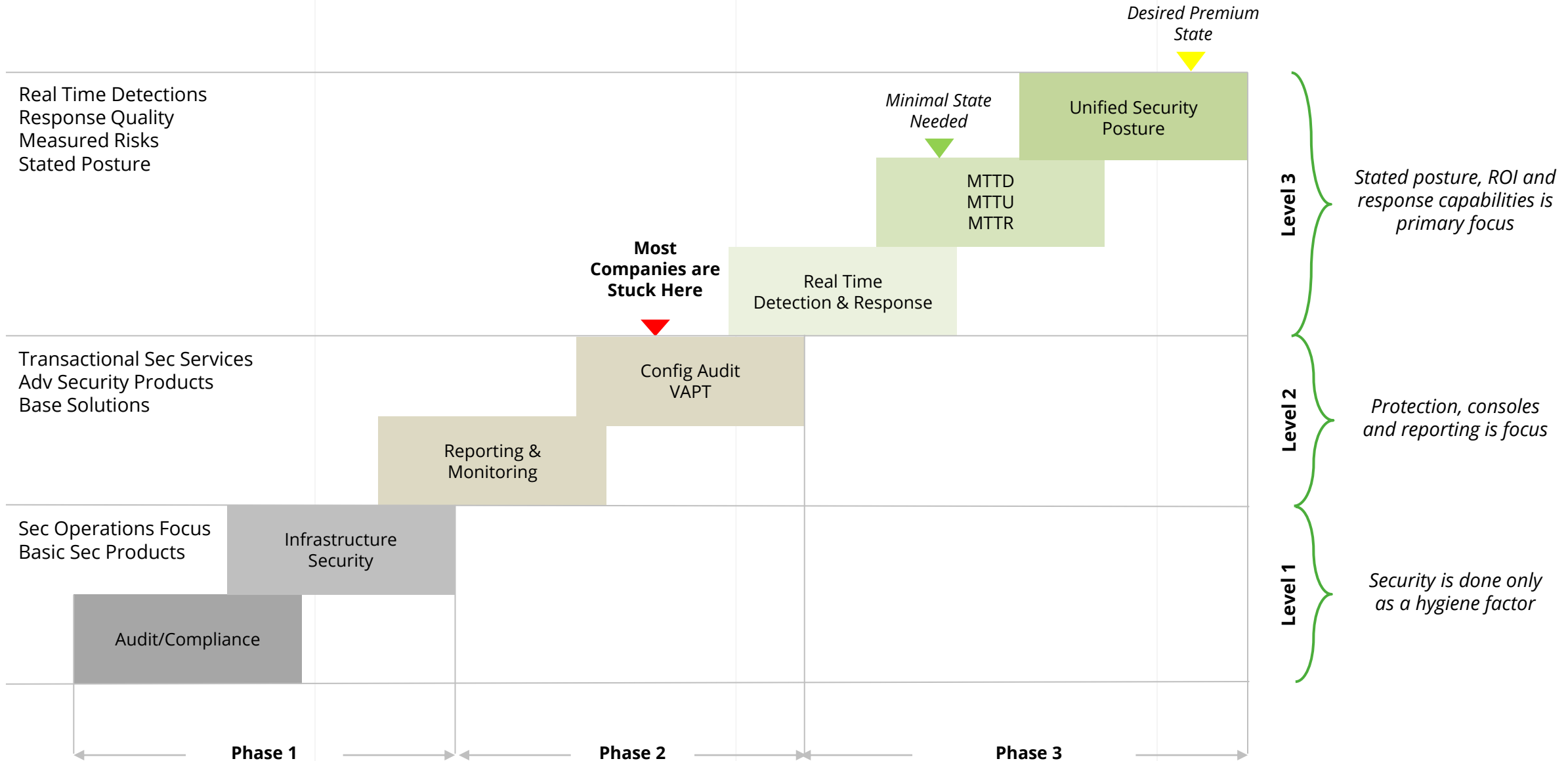
Security Operations Center (SOC)
Red Teaming
Incident Response Team



Essential:

Web App. Assmt. & Pen. Testing (**WAPT**)
Server/Device Vuln. Assmt. & Config. Audit (**VACA**)
Network Pen. Testing (**NetPT**)

Operational to Strategic Posture





Castellum Services Full Portfolio

These are subscription modeled
or annual contract modeled

Application Security

GreyBox s/w security testing
Application security design reviews
Governance/controls process adoption
Frequency based s/w testing annual contract
Fully managed AppSec programs for enterprises
DevSecOps adoption (managed or BOT modeled)

Cloud Security

Cloud Security Design
Cloud penetration testing
Cloud access implementation
Cloud SecOps and governance
Central OPS Center for Cloud security

Vulnerability Management

Network/web PT
Server configuration audit
Network device config audit
Security patch tracking/rollout
Traffic rule reviews on N/W devices
Enterprise Vulnerability Orchestration

SOC Monitoring

SOC/SIEM technology adoption
Eye-on-the-glass monitoring support
Layer 3 & 4 supplemental monitoring
Incident response support services
24x7 Managed Detection and Response



Castellum Services Full Portfolio

These are subscription modeled
or annual contract modeled

Threat Intelligence

Intel enriching & contextualization

Threat intelligence automation

Darkweb scanning/hunting

Targeted threat hunting

watchOUT

Threat Simulations

Red teaming

RT for offensive assessment

Breach simulations for readiness

Periodic assessments for response check

Enterprise Assessments

Security solutions assessment

Ent Security process assessment

People security readiness assessment

Defense assessment through offensive testing

SOC assessments for technology, process & response

Certifications Readiness

ISO 27K

GDPR

HIPPA

SOC I / SOC II

Castellum Services Previews



Application Security

Managed AppSec Programs



Cloud Security

Cloud Security Design & Governance



Threat Intelligence

Intel Enriching, Automation & Hunting



Enterprise Assessments

End-to-End Security Assessments



SOC Monitoring

Managed Detection and Response



Vulnerability Management

Enterprise Vulnerability Orchestration



Threat Simulations

Red Teaming & Breach Simulations



Certifications

ISO 27K & GDPR Readiness

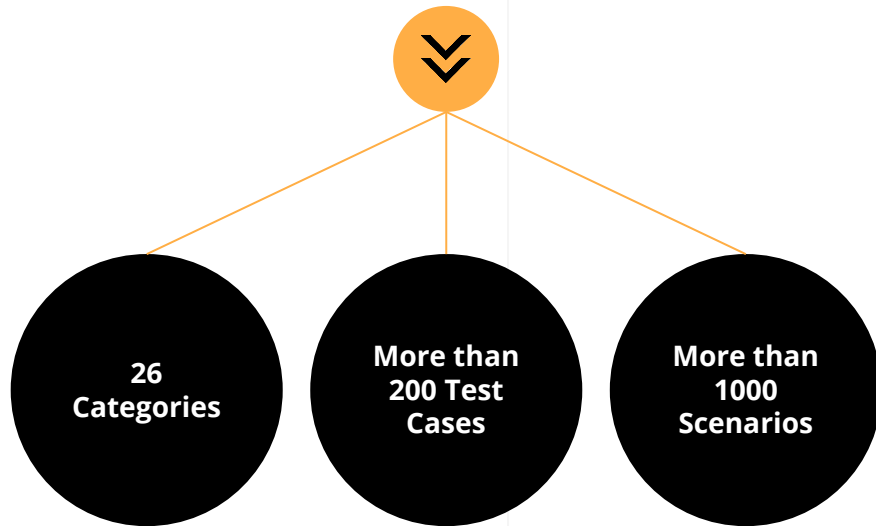


Application Security

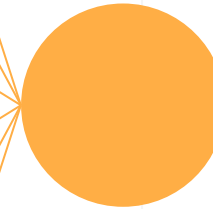
Powered by



<> 360-Degree Security



- Penetration Testing (SAST / DAST / IAST)
- Software Composition Analysis (Libraries, Open Source Vuln)
- Code Scan & Code Review (Manual and Automated Scans)
- Design Security Assessment (Selective Security Components)
- Application Data Security Review (Database & Data Security)
- Container and Server Hardening (Config, Vuln & Run Time Hardening)



Mobile
iOS
Android
Abstracted Platform
HTML 5 & Native Applications

Web Applications
Java & .Net
Angular JS and Node JS
PHP and PHP Frameworks
Middleware Frameworks

APIs
SOAP
XML-RPC
JSON-RPC
REST



Closure with Complete Remediation

"Every issue detected by our team is reported via a an IDR (Issue Details Report)"

How to
reproduce

Severity
Analysis

How to Fix
Issue

ISSUE 6 - ISSUE 6: Exploiting an Android Backup

Issue Basic Information

Issue ID : NOSL0011/POC/App-Name/M/App001/006
Application Name : App-Name (1.9.0)
Vulnerability Type : Exploiting an Android Backup
Issue Severity : **CRITICAL**

Steps to Reproduce Issue

1. To check whether any app allows the backup you need to first reverse the apk and check the AndroidManifest.xml file.
2. Check-in AndroidManifest.xml file for the attribute android:allowBackup="true" if this is present and its value is set to true it means we can backup the app internal data which resides under /data/data/<app-package>

This looks like a
You can easily fill
to others to sign,



AppSec Engagement Models

#1

Frequency AppSec Program

Recurrence based Basic Program

#2

Continuous AppSec Program

Release Model based Program Structure
Release Vuln Detection Model
Security Gate based Controls
Limited Remote Automation

#3

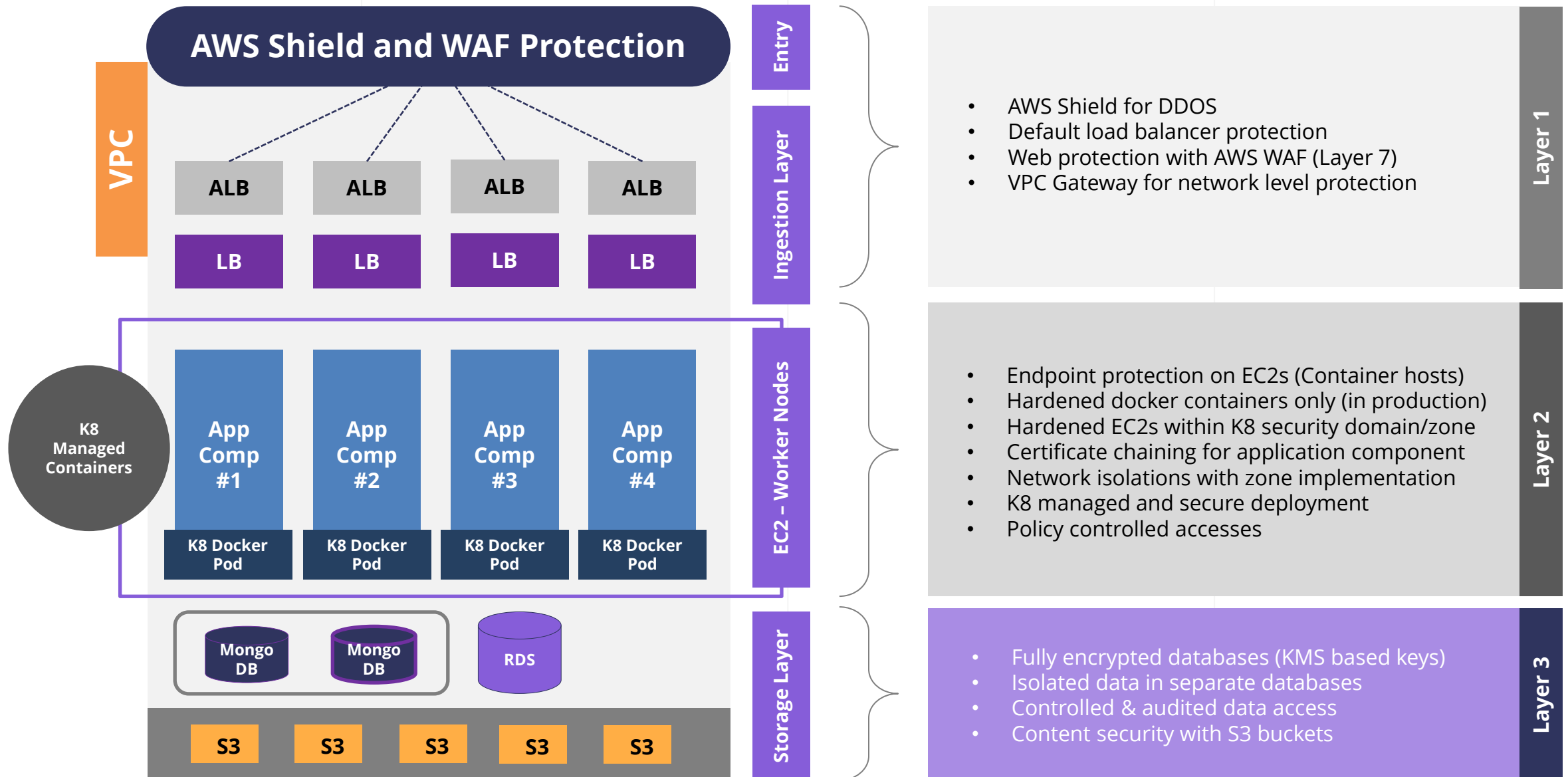
Roadmap to DevSecOps

Continuous Security Program Structure
Continuous Vuln Detection Model
Security in CI/CD based Controls
Detailed Remote Automation
Local Sec Tools Integration
Realtime Response

A grayscale background image showing a person in a business suit sitting at a desk, typing on a laptop. A calculator and a pen are also visible on the desk. The image is overlaid with a grid of thin vertical lines. A short, thick purple vertical line is positioned above the main title.

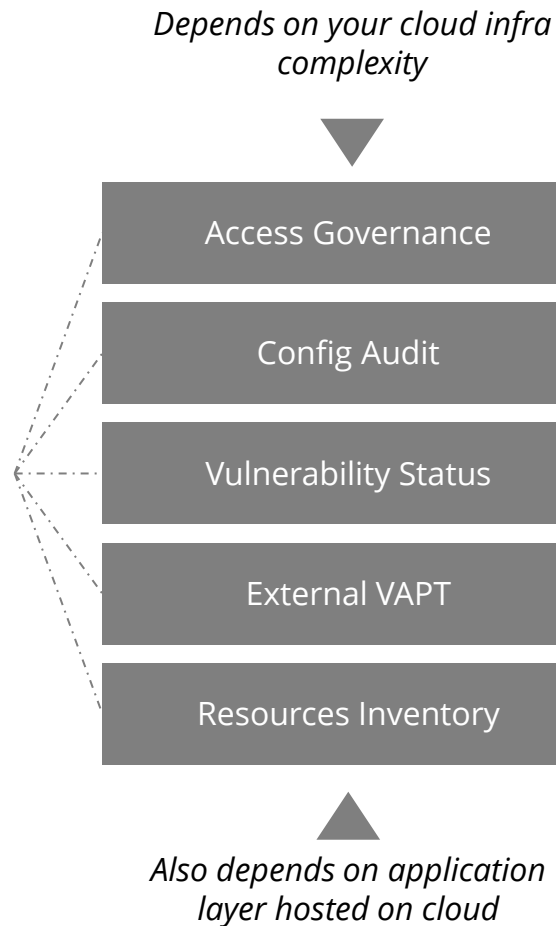
Cloud Security

Cloud Security Design Blueprint



Governance Model for Cloud

Key Governance Pivots



Frequency

Monthly/Quarterly

Monthly

Quarterly

Six Monthly

Bi-Monthly

Recurrence

Collection Templates

IAM & Direct Access

Config Collection Points

Vulnerability Checklist

VAPT Control Maps

Resource Info Points

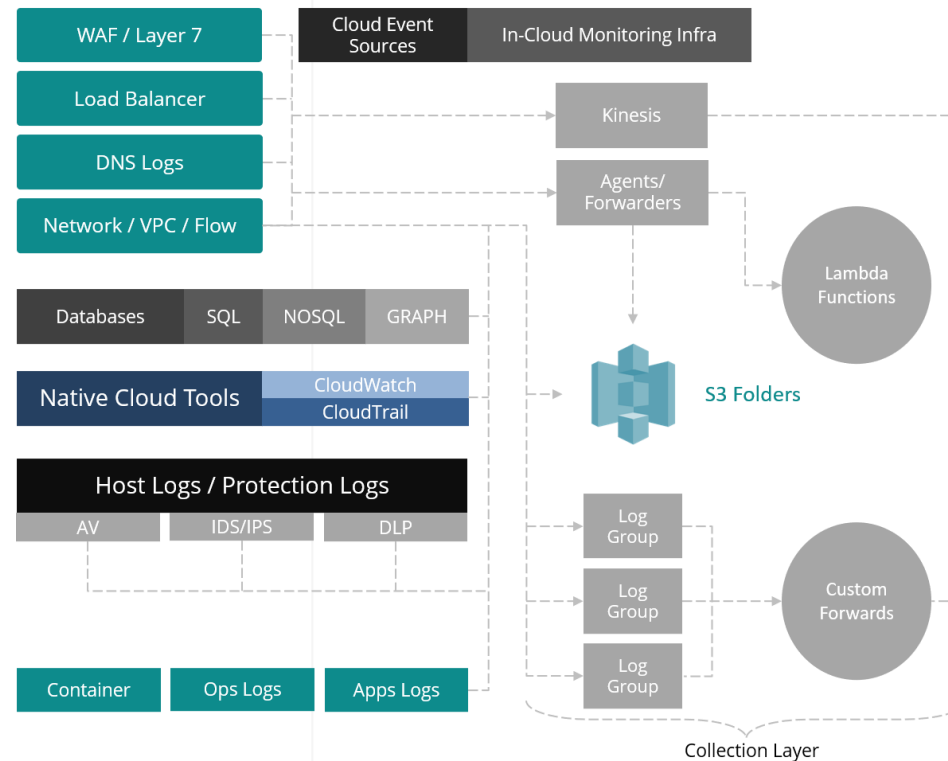
Gold Imaging

Compliance Mapping

Cloud SecOps Center

Custom Security Ops Stack (within your cloud infrastructure)

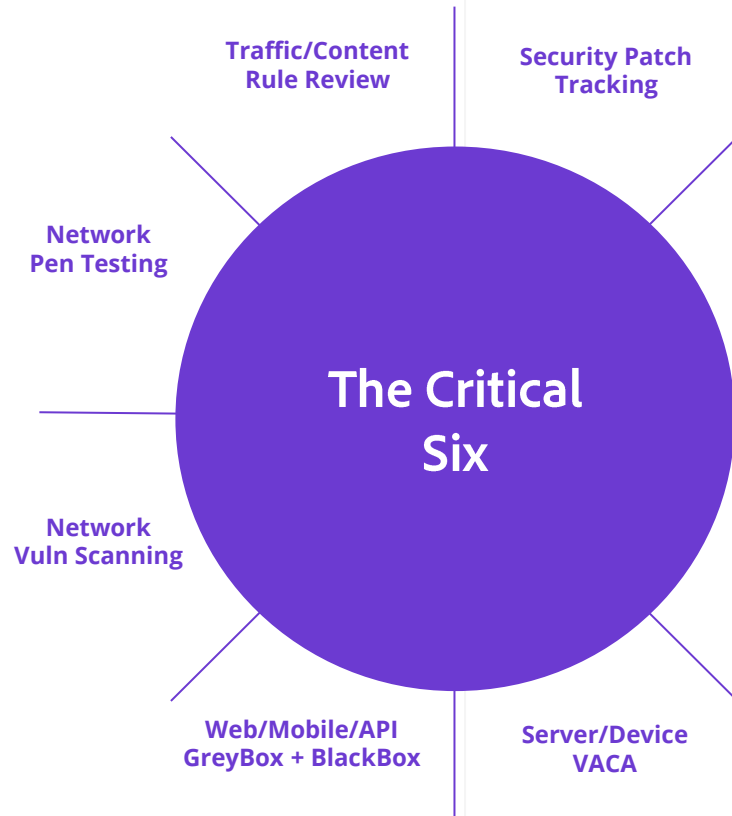
- ❖ Centralized monitoring
- ❖ Single place for all SecOps
- ❖ Central response coordination
- ❖ Centralized cloud security automation
- ❖ Secure place for cloud incident investigations



The background is a grayscale photograph of a person's hands typing on a laptop keyboard. A single, solid purple vertical line is positioned in the upper-middle section of the frame. The overall aesthetic is clean and professional.

Enterprise Vulnerability Orchestration

• Six Most Critical Elements, Fully Coordinated



- We remotely coordinate six most critical security works
- Detection, assertion, detailing & false positive removal
- Help in prioritization & remediation recommendation
- Tracking the issues reported and closure follow up
- Deep correlations, analytics, insights & reporting

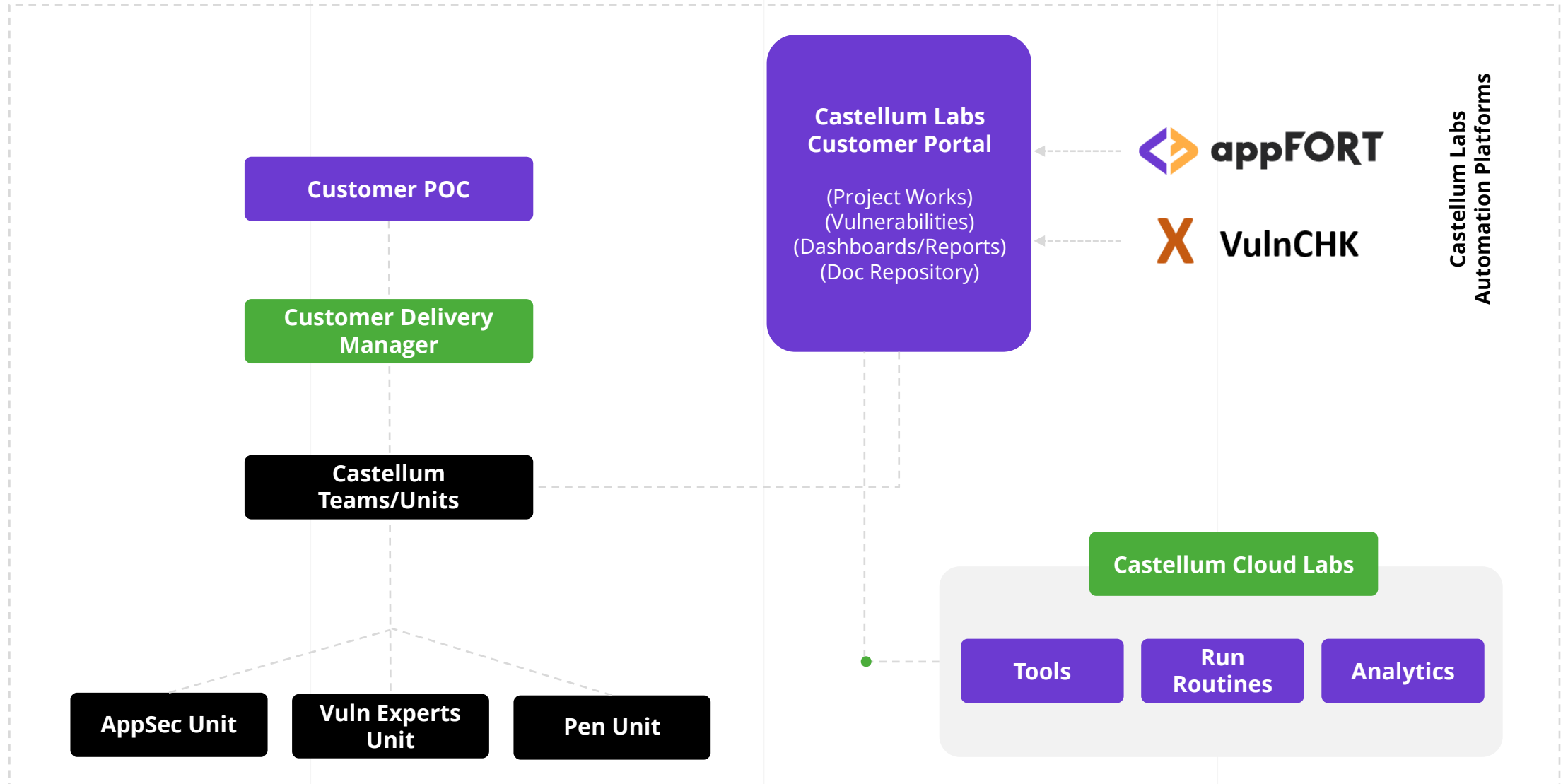
Wheel of Defense

All Critical Six

1. Network Penetration Testing/Assessment
2. Web/Mobile/API GreyBox + BlackBox
3. Server/Device Configuration Analysis
4. Security Patch Monitoring/Tracking
5. Traffic/Content Rule Review
6. Network Vuln Scanning



Automated, Fast & Accurate





True Managed Detection & Response

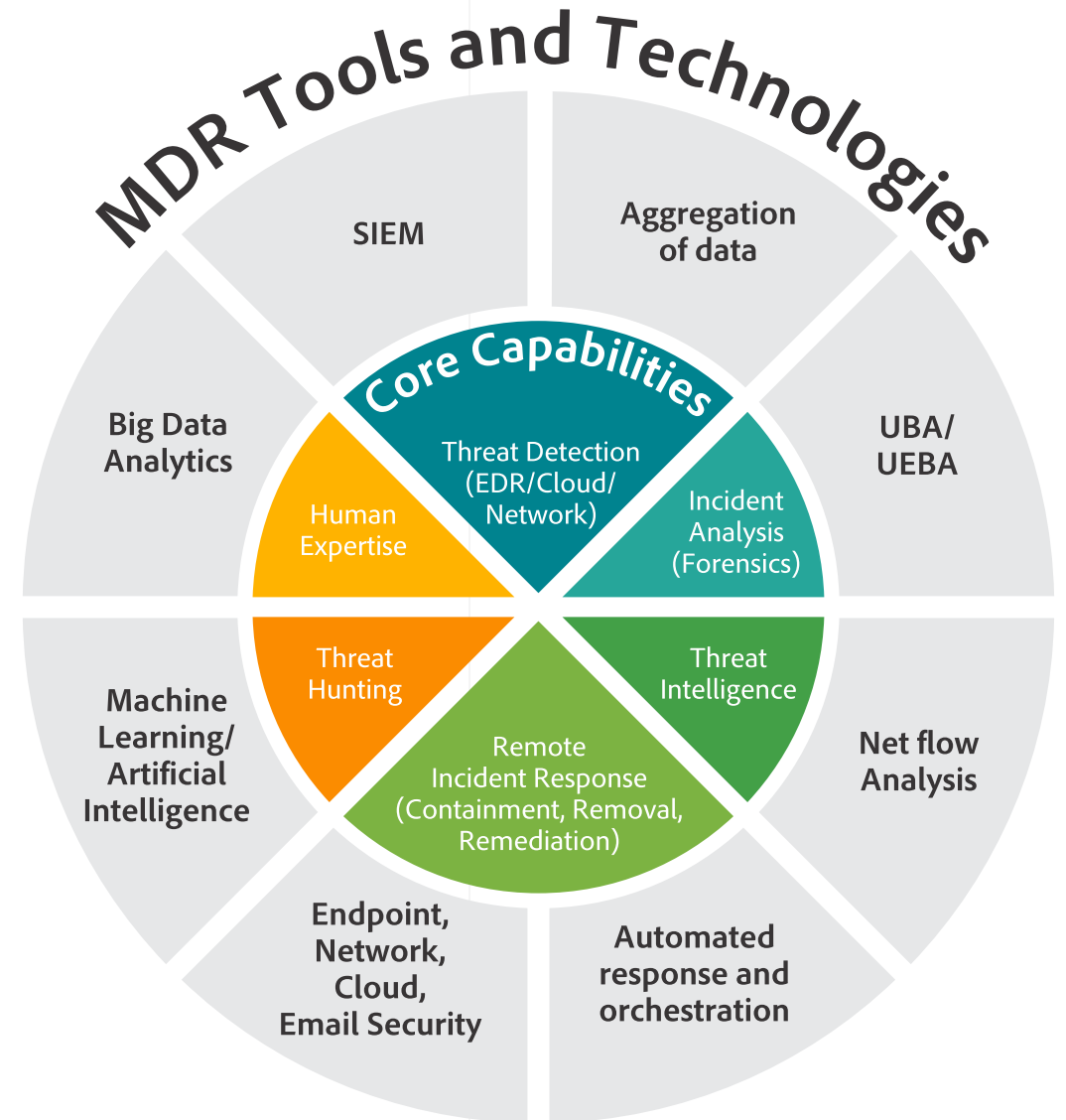
Powered by



Where we Stand Out

Automation is essential to collate, manage and classify massive amount of data. Yet platforms that rely on automation alone are always playing catch up with threat actors who constantly devise means to avoid automatic detection. We don't keep building obsolete castles with your money:

Human actors, external threat intelligence, threat hunting, manual threat detection, forensics and (what is generally poorly managed) Incident Response – manual and automated – these are our focus areas, since the tools and technologies are already built into our threatNiXD platform.



Man and Machine

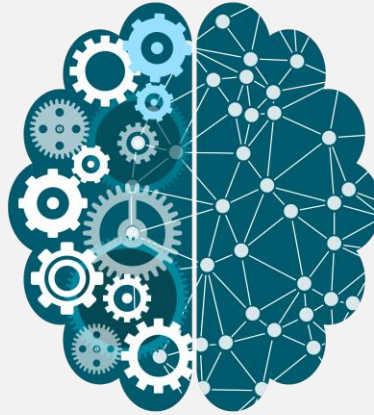
IOC ANALYSTS

Infuse Data with **Meaning**
Deep Correlation. Real Time.



ALERTS

False Negatives **Cleaned**
MITRE Mapped. Multi-channel.



DATA

Large Scale Data Collection
Redundant. Resilient. Secured.



MONITORING

Centralized Reporting
Act. Monitor. Manage. Govern.

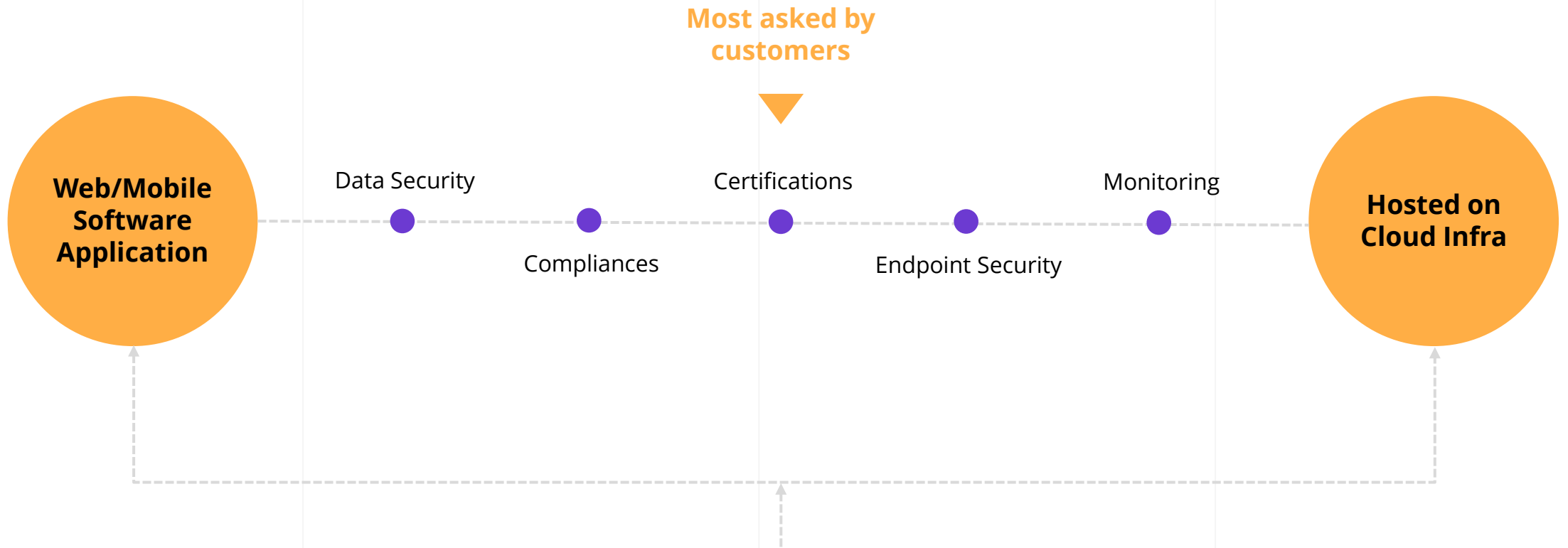
MDR on threatNiXD



A grayscale background image showing a person in a business suit sitting at a desk, typing on a laptop. A calculator and a pen are also visible on the desk. The image is overlaid with a grid of thin vertical and horizontal lines.

| Secure You Startup (SYS)

🔗 Cyber Security, a Challenge for Startups

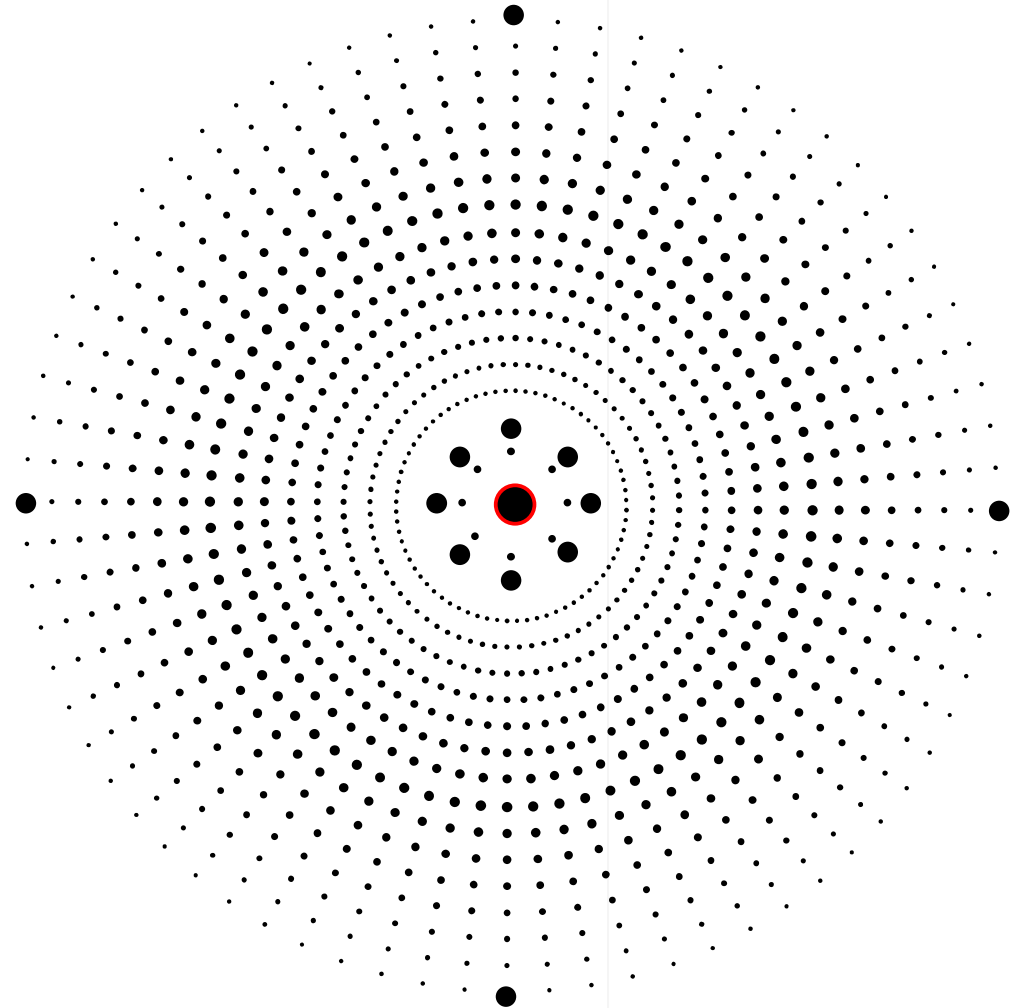


Two fixed points of **"Platform Security"** in a **"Sliding Scale of Priorities"**

• SYS, Designed to Secure Startups

SYS

Simplified Security for
Growth Startups



Engagement Models for Startups

Option #1	Option #2	Option #3	Option 4
GreyBox Good Coverage	WhiteBox Extended Coverage	Full Platform Comprehensive Coverage	Complete Assertion Secure Platform + Certification
Pen Test	Pen Test + Code Scan + Code Review + Data/Design Review	Pen Test + Code Review + Data/Design Review Server Config Hardening Cloud Security Assessment	Pen Test + Code Review + Data/Design Review Server Config Hardening Cloud Security Assessment ISO 27K and/or GDPR Certification
10 Days	22 Days	40 Days	60 Days
Manual + Tools + Platform	Manual + Tools + Platform	Manual + Tools + Platform	Manual + Tools + Platform
Remote	Remote	Remote	Remote
	Remediation Suggested	Remediation Suggested	Remediation Suggested
		S/W Remediation Fix Regressed	All Remediation Fix Regressed

A blurred background image showing a person's hands typing on a laptop keyboard. A vertical red line is positioned to the left of the main title.

External Threat Monitoring



DATA

Is my data on the Dark Web?



GAPS

What gaps exist or develop on my digital surfaces?



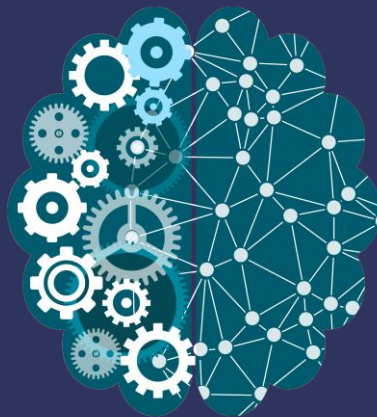
THREAT SOURCES

What threat actors and sources exist out there?



RISK

What is the risk exposure to my organization?





OSINT

Dark Web

Deep Web

Social Web

Your Attach Surfaces

watchOUT

SaaS platform for external
threats, darkweb & risks

Everyday

- We look for **Stolen and Sensitive Data** across the dark web, GitHub, your web surface
- We look for new **Phishing Domains** and check **Social Media** for handles and posts
- We keep a watch for **new vulnerabilities** due to **misconfigurations** and **exploits**
- We locate **hacked password** on dumps and **dark web** commerce sites
- We measure and report your **threat score** as well as how you compare to industry and peers
- We **proactively alert** you on **urgent** findings, out of our reporting schedule

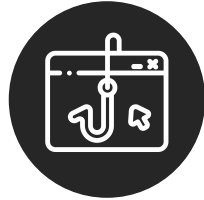


Threat Watch Coverage



Domain Watch

Domain/Sub-Domain Enumeration
Domain Threat Analysis



Phish Watch

Hunts Phishing Domains
Phishing Suspect Analysis



Cred Watch

Employee Credential Loss
Credential Stuffing Risk Analysis



Reputation Watch

Blacklists Monitoring
Detection of Malicious Content



Fake/Fraud Watch

Monitoring for Fake Sites/Pages
Detecting Misuse of Social Accounts



Social Watch

Social Surface Inventory for Company
Social Surface Check for Company



Dark Watch

Dark web Monitoring
Breach & Stolen Data Detection



git Watch

git Scan for Code Leakages
Threat Analysis of Detected Code



Leak Watch

Leakage Detection on Company Web
Threat Analysis of Leaked Info



Attack Surface Watch (Web)

Reconnaissance/Scan of Web Surface
New Gaps/Vulnerabilities Compilation



Attack Surface Watch (Network)

Reconnaissance/Scan of Net Surface
New Gaps/Vulnerabilities Compilation



Attack Surface Watch (DNS/Mail)

Reconnaissance/Scan of DNS Surface
New Gaps/Vulnerabilities Compilation



Partial Customer/Sector List

Name of Customer	Sector	Country	Area of Service
Proton	SaaS Supply Chain	SWEDEN	Application Security
Newsdesk	Media Platform	DUBAI	Application Security
Reliance	Retain POS Products	INDIA	Application Security
Reliance	Retail	INDIA	AppSec
Reliance	Online Learning	INDIA	AppSec
Reliance	Investment Mgmt	India	AppSec
Reliance Diagnostics	Pathology Labs	India	AppSec
Reliance	SaaS Platform	Australia	AppSec/Cloud
Reliance Health	Insurance	INDIA	AppSec/WatchOUT
Ministry of Internal & Security	Govt	QATAR	Network Security
Army Telecom	Telecom	UK	Network Sec / AppSec
Dr. Reddy's Lab	Pharmaceuticals	INDIA	Threat Intelligence
Reliance	SaaS HR Company	INDIA	WatchOUT

Keep in Touch.

+91 919 828 1111

enquiry@castellumlabs.com

www.castellumlabs.com

